Биткойн

Биткойн (от Bitcoin: англ. *bit* — бит и *coin* — монета) — пиринговая система электронной наличности[2][3][4], использующая одноимённую цифровую валюту[5], которую часто называют криптовалютой[6][7][8][9] или виртуальной валютой[6][10][11]. Сеть полностью децентрализована, не имеет центрального администратора или какого-либо его аналога.

Биткойны могут использоваться для оплаты товаров или услуг у продавцов, готовых их принимать. Есть возможность обмена на обычные деньги через специализированные площадки для торгов или обменники.

Одна из особенностей — эмиссия новых биткойнов. Она децентрализованная, лимитирована по объёму и времени, распределяется относительно случайно среди желающих, которые используют вычислительные мощности своего оборудования для защиты платёжной системы методом proof-of-work от повторного расходования средств. Деятельность по обслуживанию системы с возможностью получить вознаграждение в форме эмитированных биткойнов и комиссионных сборов получила название майнинга (от англ. *mining* — добыча полезных ископаемых).

Базовым элементом этой платёжной системы является программа-клиент с открытым исходным кодом. С помощью сетевого протокола прикладного уровня запущенные на множестве компьютеров клиенты соединяются между собой в одноранговую сеть.

Для обеспечения функционирования и защиты системы используются криптографические методы.

1. Кириллическое написание

При употреблении названия в русскоязычных текстах часто используют один из трёх вариантов:

- транскрипция «*Биткойн*»[2][3][12], соответствующая правилам англо-русской практической транскрипции, используемой для передачи английских собственных имён, а также других лексических единиц, непосредственно заимствуемых из английского языка (например, терминов), для которых не существует исторически сложившейся (традиционной) передачи на русский язык; применён в заявлении Банка России[11]; с 12 сентября 2014 года используется на официальном сайте.
- транслитерация «*Биткоин*»[6], соответствующая правилам транслитерации русского алфавита латиницей, применённых в обратном порядке; используется в русской локализации программы; на официальном сайте использовалась до 12 сентября 2014 года.
- оригинальное написание латиницей[8];

Разное кириллическое написание часто встречается даже в публикациях одного издателя[13][14].

2. История создания

Идеи криптовалюты «b-money» описал в 1998 году Вэй Дай (англ. *Wei Dai*) в рассылке шифропанков[15]. Также свои предложения сделал Ник Сабо (англ. *Nick Szabo*) под названием «Bitgold».

В 2008 году человеком или группой лиц под псевдонимом[16] Сатоси Накамото (англ. *Satoshi Nakamoto*) был опубликован файл с описанием протокола и принципа работы одноранговой сети[17]. По словам Сатоси, разработка началась в 2007 году[18]. В 2009 году он закончил разработку протокола и опубликовал клиент, после чего сеть была запущена.

Дальнейшую разработку организует и координирует Гэвин Андресен (англ. *Gavin Andresen*).

В мае 2010 года американец Ласло Ханеч совершил первую покупку реального товара за биткойны, купив у другого биткойнера две пиццы за 10 000 монет.[19][20]

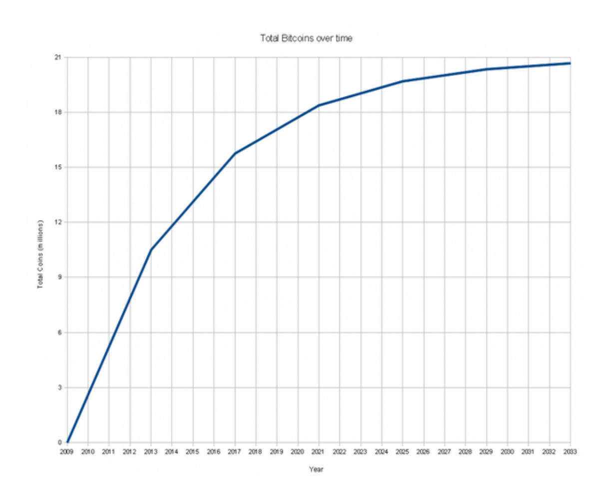
3. Описание

Платёжное средство, используемое в системе Биткойн, представляет собой цифровые монеты — криптографическую сущность, отвечающую определённым требованиям[21].

Котировка биткойн основана на доверии к нему, формируется исключительно балансом спроса и предложения, не привязана к какой-либо валюте или другому активу. В отличие от фиатных денег, система Биткойн не имеет органа (центробанка или государства), который бы стремился обеспечить ликвидность на заданном уровне, обязался сам и/или обязывал других принимать оплату в биткойнах или мог бы искус-

ственно снизить его покупательную способность путём дополнительной эмиссии. Биткойн является скорее электронной наличностью, а не долговым обязательством эмитента, что отличает его от традиционных электронных денег и безналичных расчётов.

Часто утверждается, что ограничение эмиссии является защитой от инфляции[22][6]. Ряд авторов считают, что ограниченное количество биткойнов не является достаточным условием для гарантирования тенденции роста курса, так как ещё одним необходимым условием для этого является увеличение объёма предложения товаров и услуг за биткойны и сервисов, связанных с ним[23]. То есть неспекулятивная ценность биткойнов напрямую зависит от объёма только тех товаров и услуг, которые можно будет за них приобрести, а не общемировой товарной массы.



Количество биткойнов с течением времени (годы с 2009 по 2033)

Эмиссия и оборот биткойнов полностью децентрализованы, не зависят от какого-либо регулирующего органа, объём эмиссии известен заранее. Данные о перемещении и эмиссии биткойнов хранятся в распределённой базе данных. Биткойны могут быть отправлены любому другому пользователю системы. При этом можно использовать любые дробные суммы с точностью до восьмого знака после десятичной запятой[24]. Все транзакции находятся в открытом доступе, но без раскрытия информации о реальном владельце[10]. Каждый пользователь может создать себе неограниченное количество адресов. Для повышения анонимности рекомендуется делать новый адрес получателя для каждой транзакции. Секретные ключи асимметричных пар ключей адресов пользователя хранятся в его файле кошелька wallet.dat, а соответствующие им публичные ключи используются для формирования биткойн-адресов[25].

Гипотетически есть ненулевая вероятность, что цепочка блоков будет аннулирована и в системе главной будет признана другая цепочка блоков. Вероятность такого события резко понижается с ростом длины цепочки. Но если контролировать более половины вычислительной мощности всей сети, то такая подмена возможна для любой цепочки, что гипотетически позволяет реализовать двойную трату одних и тех же биткойнов[21].

Принцип одноранговой сети и отсутствие административного центра делает невозможным государственное или частное регулирование системы, а также манипуляции с изменением суммарного количества биткойнов.

Эмиссия осуществляется автоматически: новые биткойны в качестве вознаграждения получают относительно случайным образом те, кто использует вычислительные мощности своего оборудования для поддержания работы системы Биткойн (для создания новых блоков базы). Объём эмиссии алгоритмически ограничен так, чтобы общее количество эмитированных биткойнов не превысило 21 миллиона. Первоначально размер вознаграждения за каждый созданный блок составлял 50 биткойнов. После формирования каждых 210000 блоков (приблизительно раз в 4 года) размер вознаграждения будет уменьшаться вдвое. 28 ноября 2012 года произошло первое уменьшение эмиссионной составляющей награды с 50 до 25 биткойн. На 6930000 блоке (примерно в 2131 году) эмиссия будет остановлена вовсе (размер вознаграждения $50 \to 25 \to 12.5 \to \ldots \to 0$).[26] Формирование блоков продолжится и далее, но за них уже не будет начисляться вознаграждение новыми биткойнами. Система предусматривает возможность взимать комиссию за обработку транзакций с участников. На сегодня уплата такой комиссии возможна в добровольном порядке, но не является обязательной. Предполагается, что когда вознаграждение за новый блок в форме эмиссии существенно сократится, основным источником стимулирования для формирования новых блоков станут комиссионные сборы[27].

Деятельность по созданию новых блоков с возможностью получить вознаграждение в форме эмитированных биткойнов и комиссионных сборов получила название «майнинг» (от англ. *mining* — добыча полезных ископаемых). Производимые вычисления требуются для обеспечения защиты от повторного расходования одних и тех же биткойнов, а связь майнинга с эмиссией стимулирует людей расходовать свои вычислительные мощности и поддерживать работу сети.

Майнингом можно заниматься как в одиночку (соло-майнинг), так и совместно, воспользовавшись услугами специализированных веб-служб, которые называют «пулами» (от англ. *pool* — общий фонд). Пользователи предоставляют пулу свои вычислительные мощности. Особенность задачи позволяет применить максимальное распараллеливание вычислений, когда каждый участник ищет свой вариант решения без увязки его результатов с решениями других. В свою очередь, пул, осуществляя соло-майнинг, распределяет полученные им биткойны между пользо-

вателями, в соответствии с установленными владельцем пула правилами. Основная причина объединения в пулы — уменьшение риска длительного неполучения награды. Вероятность получения награды соло-майнером в произвольный десятиминутный период приблизительно равна соотношению его вычислительной мощности к вычислительной мощности всей сети. И если это соотношение очень маленькое, то вероятность получения награды даже за длительный промежуток времени также будет низкой. В первых версиях клиента была кнопка «сгенерировать новые биткойны»[16], но после создания программного обеспечения для майнинга на видеокартах и FPGA используемый в клиенте майнинг при помощи центрального процессора оказался нерентабельным из-за слишком малой вероятности получить вознаграждение, и кнопку убрали. В настоящее время майнинг на видеокартах также стал нерентабельным, и в сети используются специально разработанные для майнинга интегральные схемы.

Передача биткойн-монет осуществляется напрямую, без посредничества каких-либо финансовых организаций. Отмена стандартных транзакций невозможна, однако возможно использование мультиподписей, в том числе для сделок с участием арбитра[28][29]. Нет обязательной комиссии, однако комиссия может быть уплачена добровольно для повышения приоритета в очереди обработки операций[30].

4. Технические подробности

4.1. Терминология

С системой Биткойн сталкиваются как IT-специалисты, так и менее квалифицированные пользователи. В связи с этим, с одной стороны, сформировалась система бытовых терминов, используемая обычными пользователями, а с другой стороны, сформировалась система терминов для специалистов, которая в основном исходит от разработчиков Bitcoin-qt и Bitcoind. Расхождения касаются наиболее часто используемых терминов. Перечислим их:

- BTC — сокращенное название единиц учёта. Используется вместо слова «Bitcoin» для однозначного указания, что имеется в виду сама цифровая валюта, а не сеть, набор алгоритмов или какая-либо другая сущность, относящаяся к данной тематике.
- bitcoind — программа (демон), в которой реализован протокол Bitcoin, используемая посредством командной строки или удаленного вызова процедур (JSON-RPC).
- Bitcoin-qt — первая программа с графическим интерфейсом Qt, совместимая с bitcoind. Система Биткойн доступна и через другие программы.
- Пара ключей — публичный и приватный ключ. Используется для генерации адреса и подписывания транзакции на перевод BTC.
- Адрес — является идентификатором, содержащим около 33 алфавитно-цифровых символов в кодировке Base58. Используется как для получения, так и для отправки BTC. Представляет собой 160-битный хэш от открытого ключа ECDSA ключевой пары.
- Кошелёк — образное название для личного хранилища BTC (account) или всё аккаунты внутри wallet.dat.
- Account — понятие в протоколе Биткойн для упрощения создания онлайн-сервиса с помощью bitcoind. Содержит некоторое количество ключевых пар и служебную информацию. Данные об аккаунтах и адресах хранятся в файле «wallet.dat». В Bitcoin-qt аккаунты отображаются как метки. Не следует путать кошелёк как весь wallet.dat, аккаунт и адрес.
- Транзакция — запись о переводе BTC с одной группы адресов (0 и более) на другую группу адресов (1 и более). Содержит подписанный отправителем хеш транзакции с помощью которой отправитель ранее получил BTC и адреса получателей BTC.
- Блок — запись в цепочке блоков(базе данных), которая содержит в себе множество ожидающих подтверждения транзакций и подтверждает их.

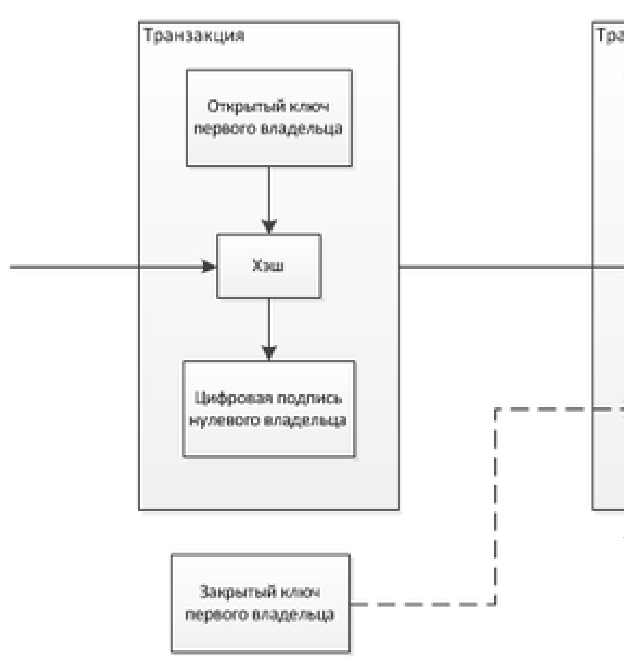
4.2. Хранение данных

БД публично хранит в незашифрованном виде информацию о всех транзакциях, подписываемых с помощью асимметричного шифрования. Для предотвращения многократной траты одной и той же суммы используются метки времени[31], реализованные путём разбиения БД на цепочку специальных блоков, каждый из которых, в числе прочего, содержит в себе хеш предыдущего блока и свой порядковый номер. Каждый новый блок осуществляет подтверждение транзакций, информацию о которых содержит и дополнительное подтверждение транзакций во всех предыдущих блоках цепочки. Для уменьшения размера БД используется древовидное хеширование[32].

Для более наглядного объяснения механизма работы платёжной системы Сатоси Накамото ввёл понятие «цифровая монета»[33], определив его как цепочку цифровых подписей. Исходя из данного определения, каждая монета имеет свой собственный номинал. Каждому биткойн-адресу может сопоставляться любое количество монет. При помощи транзакций

монеты можно делить и объединять, при этом их суммарный номинал за вычетом комиссии сохраняется.

4.3. Транзакции



Когда один пользователь передаёт некую сумму другому пользователю, он создаёт новую транзакцию, которая содержит хеш предыдущей транзакции, подписанный им, и публичный ключ следующего владельца[34]. Затем эта информация широковещательным запросом отправляется в сеть. Остальные узлы сети проверяют подписи, прежде чем принять транзакцию к обработке.

Транзакции поддерживают множественные входы (результаты предыдущих транзакций) и выходы (указания о получателях). В общем случае транзакция может содержать произвольное количество выходов (возможны случаи, когда необходимо передать средства нескольким получателям с помощью одной транзакции, что позволит сэкономить на комиссионных сборах). Транзакция также может содержать множество входов, которые могут являться даже совпадающими биткойн-адресами. Такое может иметь место, когда было несколько входящих транзакций на один адрес. Каждая первая и только первая транзакция в блоке не имеет входов и зачисляет вознаграждение за создание данного блока. Такая транзакция должна получить 120 подтверждений, чтобы полученные с помощью неё биткойны могли быть использованы. Значения со всех входов суммируются, и сумма распределяется по выходам. Разница между суммой на входе и суммой на выходе считается комиссией за осуществление транзакции. Размер вознаграждения, зачисляемого первой транзакцией, является суммой всех комиссий у транзакций, включённых в блок, и фиксированного значения, изначально равного 50 и уменьшающегося вдвое каждые 210000 блоков.

Транзакции обязательно содержат указания о получателях, например, биткойн-адреса или иные условия.

Большинство транзакций, имеющих входы, имеют минимум два выхода: с указателем получателя монеты с номиналом, равным отправленной сумме, и указателя на отправителя для «сдачи» — монеты с номиналом, который остался от суммарного номинала на входе за вычетом комиссии. «Bitcoin-qt» отправляет каждую сдачу на новый биткойн-адрес из резерва заранее созданных и скрытых от пользователя адресов. Информация о том, какая именно монета является сдачей, отсутствует в БД.

4.4. Ключи

Каждый пользователь системы может генерировать неограниченное количество пар ключей, которые хранятся в специальном файле (*кошельке*). Для создания новых пар ключей используется алгоритм ECDSA с параметрами secp256k1. Размер закрытого ключа — 256 бит, а соответствующего ему открытого ключа — 512 бит. Начиная с версии Bitcoin-Qt 0.6 используются открытые ключи в сжатом виде, которые занимают 33 байта (264 бита).[35] Создание новой пары ключей автономно и не требует соединения с сетью.

4.5. Адресация

Передача биткойнов происходит с выставлением условий для получателя. Воспользоваться суммой сможет тот, кто сможет выполнить все условия[36]. Наиболее типичным условием является использование биткойн-адреса. Переданные на адрес биткойны сможет в дальнейшем использовать только владелец соответствующего адресу секретного ключа. Но условия могут быть и другими, например, последовательное использование нескольких биткойн-адресов и/или знание праобраза хэш-значения. Биткойн-адрес генерируется на основе преобразования публичного ключа пользователя. Секретные (приватные) ключи авторизуют владельца. Биткойн-адреса не содержат персональной информации о владельце[24]. Человек может иметь множество адресов, создавая их по собственной инициативе, для чего даже не требуется подключение к интернету. Создание адреса лишь для одной транзакции или использование уникальных адресов для разных корреспондентов помогает сохранить анонимность.

Биткойн-адрес в текстовой форме представляет собой строку Base58 длиной до 34 символов, состоящую из букв латинского алфавита и цифр, напри-

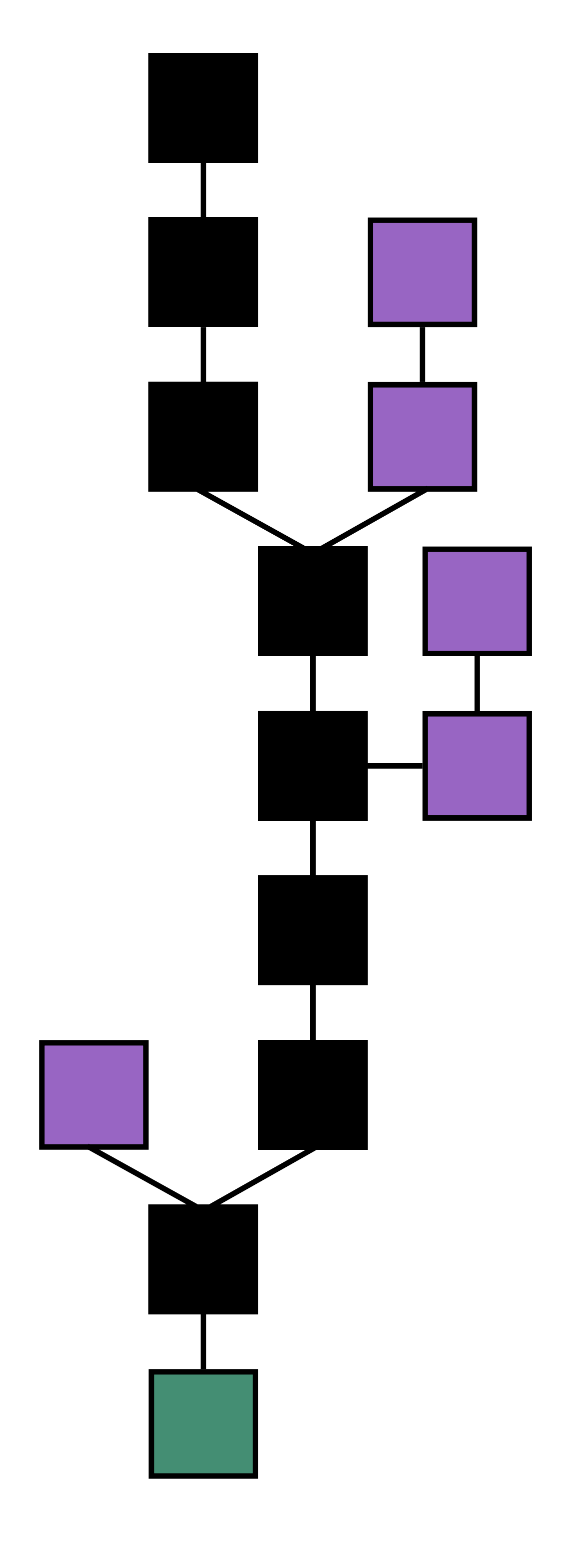
мер **175tWpb8K1S7NmH4Zx6rewF9WQrcZv245W**. Существуют варианты представления адресов в виде QR-кодов и других двухмерных штрихкодов, пригодных для считывания мобильными устройствами.

4.6. Цепочка блоков

Любые транзакции не считаются достоверными (не считаются «подтверждёнными»), пока информация о них не будет проверена и записана в специальные структуры — *блоки*. Структура и информация в блоках подчиняется заданным правилам и её можно быстро перепроверить. Каждый блок всегда содержит информацию об одном предыдущем блоке. Это позволяет все существующие блоки выстроить в одну цепочку, которая представляет собой распределённую базу данных и содержит информацию о всех совершённых когда-либо операциях с биткойнами.

Блоки одновременно формируются множеством «майнеров». Удовлетворяющие критериям блоки отправляются в сеть, включаясь в распределённую базу блоков. Регулярно возникают ситуации, когда несколько новых блоков в разных частях распределённой сети называют предыдущим один и тот же блок, то есть цепочка блоков может ветвиться. Специально или случайно можно ограничить ретрансляцию информации о новых блоках (например, одна из цепочек может развиваться в рамках локальной сети). В этом случае возможно параллельное наращивание различных ветвей. В каждом из новых блоков могут встречаться как одинаковые транзакции, так и разные, вошедшие только в один из них. Когда ретрансляция блоков возобновляется, майнеры начинаю считать главной цепочку с учётом уровня сложности хеша и длины цепочки. При равенстве сложности и длины предпочтение отдаётся той цепочке, конечный блок которой появился раньше. Транзакции, вошедшие только в отвергнутую ветку (в том числе по выплате вознаграждения), теряют статус подтверждённых. Если это транзакция по передаче биткойнов, то она будет поставлена в очередь и затем включена в очередной блок. Транзакции получения вознаграждения за создание отсечённых блоков не дублируются в другой ветке, то есть «лишние» биткойны, выплаченные за формирование отсечённых блоков не получают дальнейших подтверждений и «утрачиваются».

Таким образом, цепочка блоков содержит историю владения, с которой можно ознакомиться, например, на специализированных сайтах[37].



Основная последовательность блоков (чёрные) является самой длинной от начального (зелёный) до текущего. Побочные ветви (фиолетовые) отсекаются.

4.7. Атака «Double Spending»

Если пользователь попытается использовать ранее потраченные биткойны снова, сеть не примет его транзакцию как действительную. Но в параллельных ветках блоков могут находиться транзакции, которые по разному расходуют одни и те же начальные средства. Вероятность существования параллельных цепочек блоков крайне мала и экспоненциально уменьшается с ростом длины цепочки и количества независимых майнеров. Таким образом, чем больше под-

тверждений имеет транзакция, тем менее вероятна отмена транзакции из-за отмирания содержащей её цепочки блоков. Однако при наличии у злоумышленника контроля над достаточно большой долей суммарной мощности майнинга существует существенная (не ничтожно малая, как в обычном случае) вероятность «тайного» выстраивания длинных параллельных цепочек блоков. После их публикации в сети главной будет признана более длинная цепочка. Отмена цепочки блоков может приводить к признанию недействительными транзакций даже подтвержденных несколькими блоками и последующей повторной трате средств.

При наличии в одних руках свыше 50 % суммарной мощности майнинга такая ситуация возможна на любом уровне подтверждения (атака *«Double Spending»* или «атака 51 %»)[38]. Если подконтрольная мощность меньше 50 %, то вероятность успеха экспоненциально снижается с каждым подтверждением.

Проведение успешной атаки **не** позволяет:

- изменить размер вознаграждения за генерацию блока
- получить неограниченное количество биткойнов
- уничтожить сеть
- потратить биткойны, которые ранее не принадлежали злоумышленнику.

На начало 2013 года мощность сети составляла менее 25 THash/s, но за последующие 3 месяца выросла до 55 за счет массового распространения специализированных процессоров (ASIC), разработанных специально для майнинга в сети Биткойн.[39] В середине июля 2013 года мощность сети превысила 210,46 THash/s. К сентябрю мощность превысила 1000 THash/s, в октябре мощность удвоилась[40], а на 1 декабря 2013 года превысила 6000 THash/s[41]. При этом пользователь с наибольшей производительностью имеет менее 100 THash/s.[42]

4.8. Структура блока

Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой хеш, хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию. Первой транзакцией в блоке всегда записывается генерация новых биткойнмонет, которые в случае успешной генерации блока станут наградой пользователю за созданный блок. Далее идут все или некоторые из последних транзакций, которые ещё не были записаны в предыдущие блоки.

Созданный блок будет принят остальными пользователями, если числовое значение хеша заголовка равно или ниже определённой цели, величина которой периодически корректируется. Если блок не удовлетворяет цели, то изменяется блок служебной информации в заголовке и хеш пересчитывается. Обычно требуется большое количество попыток, так как результат хеширования (функции SHA-256) практически непредсказуем. Когда вариант найден, узел рассылает полученный блок другим подключенным узлам. Другие узлы проверяют блок. Если ошибок нет, то блок считается добавленным в цепочку и следующий блок должен включить в себя его хеш.

Величина целевого числа, с которым сравнивается хеш, корректируется через каждые 2016 блоков. Запланировано, что вся сеть будет тратить на генерацию одного блока примерно 10 минут, на 2016 блоков — около двух недель. Если 2016 блоков сформированы быстрее, то цель немного уменьшается и достичь её становится труднее, в противном случае цель увеличивается. Изменение сложности вычислений не влияет на надёжность сети Биткойн и требуется лишь для того, чтобы система генерировала блоки почти с постоянной скоростью, не зависящей от мощности сети.

4.9. Эмиссия

Система Биткойн предусматривает только одну возможность для дополнительной эмиссии — новые биткойны получает в качестве вознаграждения тот, кто сгенерировал очередной блок. Полученное вознаграждение за блоки можно использовать после получения 120 подтверждений (то есть, система разрешает тратить вознаграждение примерно через 20 часов).

Первоначально эмиссия составляла 50 биткойнов в каждом блоке. После создания 210 000 блоков (на что требуется примерно 4 года) вдвое уменьшается размер эмиссионного вознаграждения майнеров (снижается скорость эмиссии)[43]. Первое изменение произошло 2012-11-28 15:24:38 UTC: в соответствии с алгоритмом сумма вознаграждения уменьшилась до 25 биткойнов.[44] Следующий раз такое изменение произойдет ориентировочно в конце июля 2016 года.[43]

На май 2014 года в обращении находилось 12,7 миллионов биткойнов[16], что составляет более половины их максимально возможного предельного количества в 21 миллион.

Желающие получить возможно большее вознаграждение стремились задействовать как можно бóльшие вычислительные мощности. Особенность задачи позволяла применить максимальное распараллеливание вычислений. В силу специфики строения, для этого хорошо подошли графические процессоры (GPU) с небольшой дополнительной программой[45] (в сотни раз производительнее CPU[46]) и платы с FPGA (производительность сравнима с видеокартами, но превосходят их по энергоэффективности). Затем были

выпущены специализированные процессоры (ASIC), выполняющие только вычисление хешей для сети Биткойн, более производительные чем GPU и FPGA.

4.10. Сложность

За требование к хешам блоков отвечает специальный параметр, называемый «сложность». Так как вычислительные мощности сети непостоянны, этот параметр пересчитывается клиентами сети через каждые 2016 блоков таким образом, чтобы поддерживать среднюю скорость формирования распределённой БД на уровне 2016 блоков в две недели. Таким образом 1 блок должен создаваться примерно раз в десять минут. На практике, когда вычислительная мощность сети растёт — соответствующие временные промежутки короче, а когда снижается — длиннее[47]. Перерасчёт сложности с привязкой ко времени возможен благодаря наличию в заголовках блоков времени их создания. Оно записано в Unix-формате и взято по системным часам автора блока (если блок создан в пуле, то из системных часов сервера этого пула)[48].

4.11. Пулы

Для уменьшения влияния фактора удачи и более равномерного и предсказуемого получения биткойнов майнеры используют пулы[49]. Часто выплаты майнеру рассчитываются исходя из отправленных им пулу шар (shares) (блоков с хешем, который подошёл бы при сложности равной единице). В среднем нужно 2^{32} операций хеширования для нахождения одной шары[50]. Для нахождения блока в среднем требуется количество шар, равное текущей сложности.

Существуют 3 основных типа начисления наград[51]:

- Proportional — После нахождения пулом блока награда делится пропорционально вкладу каждого участника.
- PPS — Вознаграждается каждая присланная шара. Оценивается как текущее вознаграждение за блок, деленные на текущую сложность.
- Score — Оценочная система вознаграждения шар, алгоритм определяется организатором пула.

У этих типов начисления есть следующие популярные варианты:

- SMPPS — Аналогично PPS, но пул никогда не передаёт пользователям больше, чем реально получил сам. Разница между реальным получением награды пулом и вознаграждением шары в PPS, если таковая есть, компенсируется постепенно.
- ESMPPS — Аналогично SMPPS, но уравнивает приоритеты вознаграждения постоянным и новым участникам пула.
- RSMPPS — Аналогично SMPPS, но первыми в очереди на вознаграждение ставятся новые пользователи.
- PPLNS — Аналогично Proportional, но деление награды осуществляется пропорционально вкладу в последние сложность присланных на пул шар, умноженному на N, где N обычно равно 2.

4.12. Подтверждение транзакций

Обычно при получении биткойнов новый владелец не может сразу же передать их. Для уменьшения вероятности двойного использования, любая транзакция должна получить некоторое количество подтверждений. Одним подтверждением считается один новый блок, начиная с того, в котором упакована транзакция. Необходимое число подтверждений зависит от программы-клиента либо от указаний принимающей стороны.

Биткойны, полученные за создание блока, протокол разрешает использовать после 120 подтверждений[52][53]. Если учесть, что скорость появления блоков поддерживается на уровне 1 блок в 10 минут, воспользоваться комиссией можно через 20 часов после успешного начисления. Полученные от других пользователей биткойны клиент «Bitcoin-qt» позволяет использовать сразу, но у большинства получателей по умолчанию выставлено требование 6 подтверждений, то есть реально воспользоваться полученным обычно можно через час. Различные онлайн-сервисы часто устанавливают свой порог подтверждений.

4.13. Комиссионные сборы

В системе Биткойн не предусмотрено обязательных комиссионных сборов. Пользователи могут добровольно включать в платёж произвольную сумму комиссионного сбора, подавая на вход транзакции больше средств, чем на выход, что повышает приоритет обработки такой транзакции. Различные программы-клиенты имеют свои правила относительно размера и объекта комиссионных сборов. Сейчас по умолчанию Bitcoin-Qt предлагает за каждые 1000 байт длины транзакции указывать комиссию 0,0001 BTC. Средняя длина типовой транзакции составляет около 500 байт.

Комиссионный сбор достаётся узлу, сгенерировавшему блок с такой транзакцией[24]. Генерирующий новый блок может по своему усмотрению добавлять в него транзакции из очереди. Например, он может отобрать только транзакции с комиссионным сбором. По состоянию на начало 2015 года базовая реализация предусматривает, что 50 000 байт в блоке резервируется под приоритетные транзакции вне зависимости от комиссии. За счёт транзакций с комиссией величина блока может достигать 750 000 байт[54]. Таким образом, нет гарантии, что проведённая транзакция без комиссии будет включена в ближайший блок. Указание даже минимальной комиссии существенно повышает такую вероятность.

Между компьютерами сети Биткойн для защиты от слишком большого потока передаваемых данных установлено ограничение в 15 килобайт в минуту для ретрансляции информации о бесплатных транзакциях, которые ещё не включены ни в один блок.

4.14. Объём данных

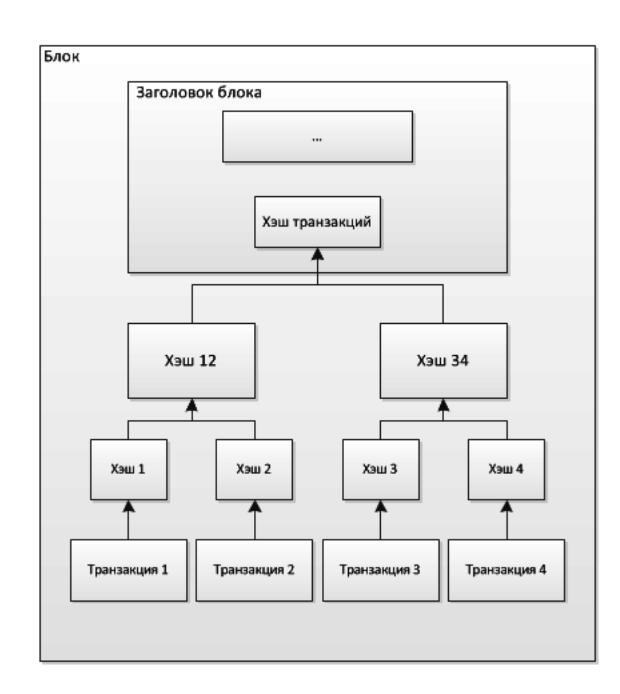


Схема получения хеша транзакций

В программах-клиентах была добавлена система, организующая записи транзакции таким образом, что пользователь может локально удалять данные из своей базы, которые ему точно не понадобятся. После того, как все транзакции с какими-то средствами были упакованы в блоки и подтверждены, предыдущие транзакции с этими средствами можно отбросить для экономии места на диске. Для того, чтобы это можно было осуществить без изменения хеша блока, транзакции хешируются с помощью TTH, и в заголовок блока помещается только результат данного хеширования.

Сейчас все пользователи официального клиентского ПО после запуска программы в первый раз получают полную базу данных (блоки без индексации и оптимизации). По состоянию на январь 2015 её размер составлял более 32 ГБ.

Заголовок блока имеет объём около 80 байт. Так как блоки генерируются примерно каждые 10 минут, то за год будет накапливаться около 4,2 Мб заголовков блоков.

4.15. Программный интерфейс

Программное обеспечение сетевого узла существует в двух видах: приложение с графическим интерфейсом и фоновое приложение. В обоих случаях оно может управляться через программный интерфейс по протоколу JSON-RPC (RFC 4627)[55] Это позволяет достаточно просто решить такие задачи, как:

- Подключить к одному узлу несколько программ-майнеров, создав собственный пул;
- Интегрировать узел с веб-сайтом, на котором используется биткойны[56];

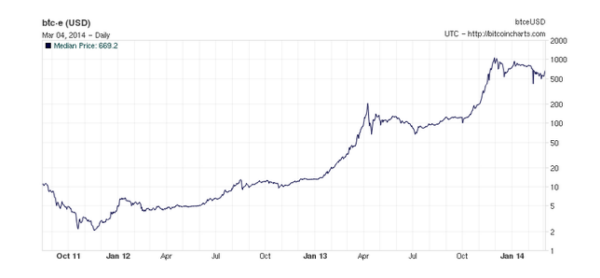
Майк Хёрн (Mike Hearn), сотрудник компании Google, в рамках программы «20 % рабочего времени сотрудника» реализовал программное обеспечение узла Биткойн на языке Java — BitcoinJ[57]. Эта реализация ограничена лишь пользовательскими функциями[58] (такой узел не может проверять транзакции и блоки, создавать блоки, а может лишь создавать новые транзакции). Это является шагом в сторону мобильных приложений, использующих биткойны.

5. Экономика

Биткойны принимаются в обмен на сетевые услуги и реальные товары[59]. Многие организации принимают пожертвования в биткойнах[60][61][62][63][64]. Предоставление возможности оплаты через биткойны может служить дополнительной рекламой, даже если такая оплата ни разу не проводилась[65].

Появилась площадка, которая на условиях маржинальной торговли предложила торговлю беспоставочными (расчётными) фьючерсными контрактами на курс «биткойн — доллар США» (BTC/USD) и на котировки других торговых инструментов.[66]

Среди пользователей принято условное обозначение **BTC**.



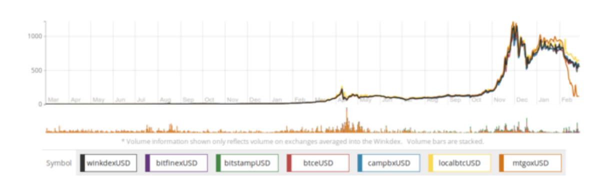
Логарифмический график обменного курса на BTC-E

5.1. Обменный курс

Важные моменты в истории системы Биткойн:

- 25 апреля 2010 года — были официально проданы первые BTC (1000 за 0,3 цента каждая).
- 10 февраля 2011 года — На Slashdot появилась новость[67] о достижении паритета между BTC и USD.
- 20 апреля 2011 года — Forbes публикует статью «Crypto Currency»[68], после чего курс BTC стал расти быстрее и к концу мая достиг 8,89 долларов.
- 1 июня 2011 года — Gawker опубликовал статью «The Underground Website Where You Can Buy Any Drug Imaginable» о подпольной торговой площадке Silk Road[69], после чего курс BTC резко подскочил.
- 9 июня 2011 года — курс биткойна достиг 29,57 доллара[70], что до 19 февраля 2013 года являлось историческим максимумом[71].
- 19 июня 2011 года — крупнейшая биткойн-биржа Mt.Gox была взломана[72], после чего курс BTC продолжил падение.
- лето 2012 года — после долгого нахождения около отметки в 5 долларов, курс начал расти.
- 28 ноября 2012 года — первое уменьшение скорости эмиссии в 2 раза.
- 22 февраля 2013 года — курс достиг отметки в 30 долларов[71], превысив максимум 2011 года.
- 1 апреля 2013 года — курс превысил отметку в 100 долларов[73].
- 10 апреля 2013 года — после очень быстрого роста, курс превысил 266 долларов, после чего произошёл резкий обвал до уровня 50 долларов[74].
- 19 ноября 2013 года — курс достиг 900 долларов, после чего резко снизился[75]. Стоит отметить, что цена одного BTC на различных биткойн-биржах в момент пика значительно отличалась. На BTC-е курс достиг лишь отметки в 823 доллара, а на китайских биткойн-биржах достигал эквивалента 1200 долларам.
- 28 ноября 2013 года — курс превысил отметку в 1000 долларов.[76]
- 5-8 декабря 2013 года — курс упал с 980 до 576 долларов после того, как ЦБ Китая запретил китайским банкам и другими финансовым учреждениям осуществлять операции с биткойнами, после чего сразу же восстановился до 800 долларов.
- 11 апреля 2014 года после постепенного падения в течение 4-х месяцев курс снизился до уровня 340 долларов.

5.1.1. Mt.Gox



Обменный курс Bitcoin/USD на Mt.Gox и рыночный курс.

Mt.Gox («Magic: The Gathering Online eXchange»[77]) — первая и наиболее известная площадка купли-продажи биткойнов, обанкротившаяся в феврале 2014 года. Расположена в Японии. В конце февраля 2014 года торги остановлены[78] в связи с кражей у Mt.gox крупной суммы биткойнов и фактическим банкротством[79]. Торги велись с использованием счёта трейдера в национальной валюте. Торговля напрямую между национальными валютами не поддерживалась. Владельцы Mt.Gox оставляли за собой право блокировать учётные записи трейдеров, не подтвердивших свою личность.

До февраля 2014 год обменный курс биткойна к доллару был выше, чем на остальных аналогичных площадках, в связи с задержками вывода средств в долларах, возникших из-за действий властей США. По состоянию на февраль 2014 года на Mt.Gox полностью закрыт вывод биткойнов, а для вывода любой суммы в долларах стала требоваться обязательная идентификации личности, которую владельцы Mt.Gox начали запрашивать повторно. Поэтому котировки Mt.Gox не отражали реального рыночного курса[80]. В феврале 2014 года стало известно, что на Mt.Gox использовалось уязвимое программное обеспечение, которое было написано владельцами для внутренних нужд. Уязвимость в ПО позволила злоумышленникам незаметно красть биткойны у Mt.Gox. После закрытия вывода биткойнов курс на Mt.Gox обрушился, поскольку затруднённая возможность вывода в долларах осталась, в то же время ре-

альный рыночный курс биткойна лишь незначительно снизился.

20 марта 2014 г. гендиректор компании Марк Карпелес объявил, что ранее считавшиеся утерянными 200 000 биткойнов на общую сумму около 116 млн долларов оказались в электронном кошельке старого формата, который использовался до июня 2011 года. Из соображений безопасности эту сумму перевели в оффлайн-кошельки и проинформировали об этих транзакциях судебные и надзорные органы, занимающиеся кражей у Mt.Gox биткойнов и банкротством. Таким образом, число исчезнувших биткойнов сократилось с 850 000 до 650 000[81].

15 апреля 2014 года Mt.Gox подала в суд Токио заявление о ликвидации[82].

5.1.2. BTC-E

BTC-E является крупной площадкой по обмену биткойнов. Имеется обмен на доллары США, российские рубли и евро, между которыми поддерживается также обмен напрямую по внутреннему курсу, который иногда может сильно отличаться от рыночного.

Есть торговый API. В отличие от Mt.Gox, при регистрации нет требования идентификации личности.

В ноябре 2013 года доля торгов на этой площадке достигала около 30 %, сравнявшись с площадкой Mt.Gox.

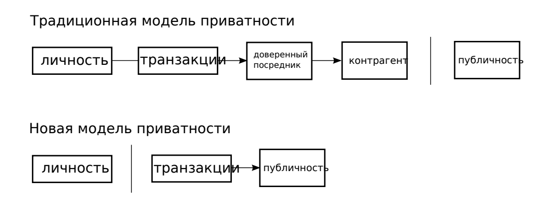
5.1.3. WebMoney

16 мая 2013 года популярная платёжная система WebMoney объявила о вводе титульных знаков «WMX» номинированных в биткойнах, находящимися на хранении у гаранта. 1 WMX эквивалентен 0,001 BTC[83] При передаче WMX внутри Webmoney, транзакций в системе Биткойн не проходит. Работа с WMX аналогична работе с другими титульными знаками WebMoney, и поэтому не требует ждать подтверждений (создания новых блоков) и позволяет возвращать ошибочные или мошеннические транзакции. В то же время система WebMoney менее анонимна, чем система Биткойн и для полноценной работы требует указания достоверных паспортных данных. Возможен обмен WMX на другие титульные знаки через сервисы партнеров WebMoney.

С другими площадками обмена можно ознакомиться на Bitcoin Wiki.

5.2. Конфиденциальность

В системе Биткойн история всех транзакций публично доступна. Можно проследить все операции с момента генерации до текущего псевдонимного адреса.



Сравнение традиционной модели приватности с моделью приватности в системе Биткойн.

В своей статье[30] Сатоси Накамото отмечает, что анонимно созданные биткойн-адреса помогают сохранить конфиденциальность. Так же рекомендуется использовать новые адреса для каждой новой транзакции, чтобы избежать сопоставления их с одним владельцем. Фергал Рид и Мартин Харриган провели анализ степени анонимности в системе Биткойн. Они показали, что с помощью общедоступной информации возможно связать многие открытые ключи как друг с другом, так и с какой-либо внешней идентифицирующей информацией. Также авторы статьи замечают, что обменники, магазины и хранилища кошельков способны выявлять и отслеживать значительную часть персональной активности, опираясь на e-mail, IP, номера кредитных карт и т. п.[84].

Дополнительную анонимность при использовании системы Биткойн можно обеспечить через сеть Tor.

Также для сохранения конфиденциальности может быть применён «биткойн-миксер», который выполняет смешивание монет разных пользователей.

5.3. Сайты с бесплатными биткойнами

К концу 2014 года существовало множество сайтов (англ. *Bitcoin faucet*), которые педлагают всем желающим регулярно получать небольшое количество бесплатных сатоши в обмен на выполнение простых задач, например, клик на рекламном банере, решение капчи, просмотр веб-страницы в течение определённого времени. Эти сайты обычно предлагают общую информацию о биткойнах. При регистрации надо сообщить номер кошелька для зачисления полученных сатоши. куда будут зачисляться

Типичный размер выплат за транзакцию составляет менее 1000 Сатоши, хотя многие сайты в лотерейном порядке разыгрывают достаточно большие выплаты. Обычно сайты учитывают начисления в собственной системе, где они суммируются для достижения более крупной суммы, которая будет отправлена на биткойн-кошелёк. Это делается для снижения накладных расходов сборов.

Появились сайты, при входя на которые происходит

одновременное подключение сазу к нескольким сайтам, которые начисляют бесплатные сатоши. Это позволило экономить время на переподключениях.

Бизнес-модель сайтов с выплатой бесплатных сатоши строится на получении дохода от баннерной рекламы и последующем распределении между зарегистрированными пользователями части этого дохода.

Многие подобные сайты имеют систему реферальных выплат.

6. Отзывы общественных деятелей

- Марк Андрессен — автор первого графического интернет-браузера NCSA Mosaic, один из основателей фонда венчурного фонда Andreessen Horowitz в кремниевой долине и инвестор в стартапы, связанные с биткойнами, — сравнивает систему Биткойн в 2014 году с Интернетом в 1993 году и персональными компьютерами в 1975 году[85][86], а также говорит:

  > На фундаментальном уровне Биткойн является прорывом в области компьютерных наук — тех, что опираются на 20 лет исследований криптографических валют и 40 лет работы в области криптографии тысяч исследователей по всему миру.
  >
  > — Марк Андрессен

- Основатель пиратской партии Швеции Рикард Фальквинге в 2011 году высказывал схожую мысль[87]:

  > Я предвижу, что Биткойн станет широко использоваться где-то к 2019 году. Мой прогноз основан на развитии других новаторских технологий. Например, блоггинг появился в 1994, но пришёл в широкие массы в 2004; файлообмен появился ещё в 1989, но только с появлением «Напстера» в 1999 он пришёл к массам. Потоковое видео появилось в 1995, причём поначалу, только в порноиндустрии, в 2005 появился «YouTube» — и всё переменилось, настолько он был удобен. В этом нет ничего плохого, это просто наблюдение, что любой новаторской технологии с момента внедрения до созревания и удобства в использовании, необходимого для выхода в широкие массы около десяти лет.
  >
  > — Рикард Фальквинге; Rick Falkvinge — шведский предприниматель в отрасли информационных технологий, политик, основатель Пиратской партии Швеции.

  В 2013 году он же в своей авторской колонке на сайте rt.com поясняет, почему Эдвард Сноуден и криптовалюта Биткойн являются, по его мнению, одними из главных трендов 2013 года:

  > Биткойн изменит общество сильнее, чем интернет. Но это станет очевидным не ранее 2025 года, а более вероятно — 2035. Так же, как и польза разоблачений Эдварда Сноудена пока не может быть оценена по достоинству в 2013 или 2014 годах.
  >
  > — Рикард Фальквинге

- Глава Банка Японии Харухико Курода сказал, что банковский Институт денежных и экономических исследований сейчас проводит изучение Биткойн[88].

  > По сравнению с традиционными способами денежных переводов и существующими электронными деньгами, Биткойн имеет как похожие, так и отличные черты.
  >
  > — Харухико Курода

- Экс-глава ФРС США Алан Гринспен 5 декабря 2013 года в интервью агентству Bloomberg заявил, что считает Биткойн «мыльным пузырём», так как, по его мнению, биткойн-монеты не имеют никакой реальной ценности[89]:

  > У валюты должна быть своя собственная ценность. И нужно сильно напрячь воображение для достижения умозаключения, что биткойн обладает внутренней стоимостью. У меня это не получилось.
  >
  > — Алан Гринспен

- Глава Сбербанка Герман Греф на форуме в Давосе сказал[90]:

  > Криптовалюты — это очень интересный международный эксперимент, который ломает парадигму

> валютной эмиссии. И их определено не стоит запрещать, но следует попытаться понять, изучить и, возможно, начать правильно регулировать.
>
> — Герман Греф

Он так же направил письма в администрацию президента РФ, Центробанк и Министерство финансов с просьбой не накладывать ограничения на использование виртуальных валют и электронных платёжных систем, назвав подобное «колоссальным шагом назад»[91].

- Американские бизнесмены Братья Уинклвосс прогнозируют, что котировка биткойна в будущем достигнет 40 тыс. долларов.[92].

- Партнёр Andreessen Horowitz Крис Диксон прогнозируют котировку в будущем до 100 тыс. долларов и[93] сравнивая Биткойн с интернет-доменами говорит:

> В 1993 году было бы абсурдно утверждать, что некоторые доменные имена когда-нибудь будут стоить 10 миллионов долларов.
>
> — Крис Диксон

7. Правовой статус

В разных странах отношение к системе Биткойн сильно различается:

7.0.1. Германия

В конце августа 2013 года Министерство финансов ФРГ сделало заявление о том, что биткойн не может быть классифицирован как электронная или иностранная валюта, а больше подходит под определение *частные деньги*, с помощью которых могут осуществляться *многосторонние клиринговые операции*.[94]

7.0.2. Хорватия

Национальный банк Хорватии считает, что биткойн является законным в Хорватии, но его не следует рассматривать как электронные деньги, хотя он имеет некоторые сходства с ними. Криптовалюты могут легально использоваться в стране, хотя не могут считаться законным платёжным средством то есть продавцы не обязаны их принимать в Хорватии наравне с местной валютой[95].

7.0.3. Дания

Дания[96].

7.0.4. Швеция

Швеция[97][98].

7.0.5. Южная Корея

Южная Корея[99]

7.0.6. Япония

До марта 2014 года Банк Японии не имел каких-либо планов относительно регулирования оборота биткойнов[88]. Однако после краха Mt.Gox, базировавшейся в Токио, власти Японии объявили о необходимости регулирования данного рынка. Ожидается разработка норм налогообложения.[100]

7.0.7. Таиланд

По заявлению компании из Бангкока «Bitcoin Co. Ltd.», Банк Таиланда хоть и не признал биткойн как самостоятельную валюту, но заявил, что для операций с ним требуется лицензия на право проведения валютообменных операций, отказавшись её выдать. С 29 июля 2013 компания приостановила свой обменный сервис. На сайте компании со ссылкой на представителя Банка Таиланда объявляется, что «из-за отсутствия законных оснований, в Таиланде являются незаконными покупка/продажа биткойнов, покупка/продажа любых товаров или услуг в обмен на биткойны, отправка биткойнов за пределы Таиланда или приём биткойнов извне Таиланда».[101] На официальном сайте Банка Таиланда по состоянию на 2 августа 2013 года подобного заявления не обнаружено. 15 февраля 2014 года компания получила письмо от Банка Таиланда с разъяснением, в котором говорилось, что обмен биткойнов не попадает под тайское валютное законодательство и регулирование Министерства финансов, так как для обмена не предлагаются иностранные валюты, после чего сервис сразу открылся[102]. Через некоторое время Банк Таиланда прислал письмо с дополнительным разъяснением, в котором говорится, что хоть сервис и обменивает только биткойны и баты, биткойны потом можно обменять на иностранную валюту, значит с обменом иностранной валюты он всё же связан. Сервис продолжил работу, внеся в пользовательское соглашение условие, согласно которому пользователи обязуются не обменивать полученные через сервис биткойны на иностранные валюты[103].

7.0.8. Китай

5 декабря 2013 года Народный банк Китая запретил китайским финансовым компаниям проводить операции с биткойнами.[104] В заявлении указано, что биткойн не является валютой в реальном смысле этого слова. Финансовым компаниям запрещены не только прямые операции с биткойнами, но и публикация котировок или страхование финансовых продуктов, связанных с биткойном. В то же время физические лица могут свободно участвовать в интернет-транзакциях на свой страх и риск. Биткойны при этом рассматриваются как некий товар, но не денежные средства.

В конце марта 2014 года Народный банк Китая выпустил циркуляр, согласно которому к 15 апреля 2014 года китайские банки и платёжные системы должны закрыть счета пятнадцати китайских веб-сайтов, которые продают биткойны. Неповиновение будет караться, но Народный банк Китая не уточняет, как именно.[105]

7.0.9. Евросоюз

ЕЦБ[106]

7.0.10. США

В официальных отчётах Всемирного банка и ФБР биткойн считают «виртуальной валютой»[10] По классификации комиссии по финансовым преступлениям (англ. *FinCEN*) при министерстве финансов США биткойн относят к «децентрализованным виртуальным валютам»[107].

В марте 2013 года FinCEN объявила о том, что операции по обмену любых криптовалют на фиатные деньги должны регулироваться так же, как и операции по обмену фиатных денег между собой (например, доллары на евро).[108] Не только биткойн-биржи, но и обменные пункты должны зарегистрироваться в качестве поставщиков финансовых услуг (англ. *Money Service Business*) и сообщать о подозрительных транзакциях в органы правопорядка. Несколько американских обменных сервисов, например BitInstant, были вынуждены закрыться до получения соответствующих финансовых лицензий. В ноябре 2013 в Сенате США проходили слушания по поводу Биткойн, в ходе которых было решено не запрещать хождение криптовалют, а работать над регулированием этого бизнеса.[109]

В августе 2013 года судья Восточного округа штата Техас (США) принял решение: так как биткойны можно использовать в качестве денег для оплаты за товары или обменять на обычные валюты, такие как доллар США, евро, иена или юань, то биткойн является валютой или формой денег[110].

25 марта 2014 года Служба внутренних доходов США выпустила руководство по налогообложению операций с биткойнами и другими виртуальными валютами.[111] Для целей уплаты федеральных налогов биткойны рассматривается как имущество, то есть те, кто приобретает биткойны в качестве инвестиционного инструмента, при продаже биткойнов получат прибыль от «прироста капитала», а не прибыль от «курсовой разницы». Реализуя товары и оказывая услуги в обмен на биткойны, налогоплательщик получает прибыль, которая исчисляется по курсу биткойна к доллару США на день оплаты. Приобретая товары и услуги за биткойны, налогоплательщик несёт расходы, которые также можно учесть при расчёте налоговой базы (для расчёта также используется курс биткойна к доллару США на день оплаты). Прибыль от выпуска биткойнов облагается налогами. Высокая волатильность курса биткойна может повлечь налоговые обязательства для тех, кто расплачивается биткойнами за товары и услуги (в частности, обязанность уплатить налог на прибыль от прироста капитала).[112]

7.0.11. Швейцария

В декабре 2013 года швейцарским парламентом был предложен постулат, согласно которому биткойны следует рассматривать как иностранную валюту[113]. Постулат был подписан 45 из 200 членами парламента, и окончательное решение будет принято в начале 2014 года.

7.0.12. Сингапур

В начале января 2014 года стало известно, что налоговые органы Сингапура приравняли операции с биткойнами к операциям, облагаемым налогом на товары и услуги.[114][115] Стандартный налог на прибыль планируется взимать с компаний, занимающихся покупкой и продажей биткойнов. Не будет облагаться налогами долгосрочное инвестирование в биткойны, приравненное к вложениям в капитал. При обмене биткойнов на реальные товары и услуги будет взиматься налог на товары и услуги 7 % (для нерезидентов налог на товары и услуги не возникает)[116]. Налогом на товары и услуги не будет облагаться приобретение за биткойны виртуальных товаров и услуг, таких как внутренние покупки в приложениях (in-app purchases)[117].

13 марта 2014 года Денежно-кредитное управление Сингапура объявило о намерении урегулировать деятельность посредников, осуществляющих операции с виртуальными валютами (подразумевая под ними в том числе биткойн)[118]. Таких посредников, производящих обмен виртуальных валют на реальные, обяжут идентифицировать своих клиентов и сообщать в

соответствующее ведомство о подозрительных транзакциях. В целом, к посредникам будут предъявляться те же требования, что и к предприятиям, занимающимся обменом реальных валют, а также обеспечением денежных переводов. Цель указанных мер — минимизировать риски, связанные с отмыванием денежных средств и финансированием терроризма, проистекающие из анонимной природы виртуальных валют.

7.0.13. Болгария

2 апреля 2014 года болгарское Национальное Агентство по Доходам опубликовало на своем сайте новость, согласно которой доходы от сделки с биткойнами должны декларироваться и облагаться налогом. Налоговая служба признала такие доходы доходами от финансовых активов и постановила, что они облагаются налогом по ставке 10 %.[119]

7.0.14. Российская Федерация

27 января 2014 года Пресс-служба Банка России опубликовала информацию «Об использовании при совершении сделок „виртуальных валют“, в частности, Биткойн»[11]. В ней Банк России предупредил, что в связи с отсутствием обеспечения и юридически обязанных субъектов операции по «виртуальным валютам» являются спекулятивными. В связи с анонимным характером деятельности по выпуску «виртуальных валют», неограниченным кругом субъектов, и по их использованию для совершения операций граждане и юридические лица могут быть, в том числе непреднамеренно, вовлечены в противоправную деятельность, включая легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма. Предоставление российскими юридическими лицами услуг по обмену «виртуальных валют» на рубли и иностранную валюту, а также на товары (работы, услуги) будет рассматриваться как потенциальная вовлечённость в осуществление сомнительных операций в соответствии с законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма.

15 апреля 2014 года инициативная группа заявила о создании общественной организации «Национального фонда развития криптовалют». Главную цель создатели видят в пропаганде криптовалют.

В начале июля 2014 года в рамках Международного банковского конгресса первый заместитель председателя Банка России Георгий Лунтовский высказался о том, что за системой Биткойн наблюдают, вопрос изучается, возможно в будущем появится законодательное регулирование[120].

9 августа 2014 года, выступая в Санкт-Петербурге на #CryptoForum, 1-й международной конференции «Bitcoin и криптовалюты: перспективы развития в России», руководитель департамента информации и коммуникаций Международного учебно-методического центра финансового мониторинга (МУМЦФМ) при Росфинмониторинге Евгений Воловик, являющийся также членом международной рабочей группы, разработавшей в июне 2014 года ключевые определения виртуальных, централизованных и децентрализованных валют (оригинал документа), категорично заявил, что «Биткойн не является денежным суррогатом», но и добавил, что криптовалюты попали под внимательный присмотр международной организации ФАТФ, занимающейся борьбой с отмыванием денег и финансированием терроризма. Воловик также заметил, что в России уже ведется одно или несколько дел, связанных с отмыванием средств посредством Биткойн, но сообщить подробности отказался.

На основании решения Невьянского городского суда Свердловской области 13 января 2015 года в единый реестр запрещённых сайтов было включено 7 сайтов, связанных с тематикой биткойн, в том числе сайт bitcoin.org[121]. Это привело к блокированию доступа к сайтам со стороны российских провайдеров, в том числе мобильными операторами. Первоначально причина не сообщалась. Позже стала доступна копия судебного решения[122], согласно которому

> Свободное распространение информации об электронной валюте обуславливает активное использование криптовалют в торговле наркотиками, оружием, поддельными документами и иной преступной деятельности. Данные факты, а также возможность бесконтрольного трансграничного перевода денежных средств и их последующего обналичивания, служит предпосылками высокого риска потенциального вовлечения криптовалют в схемы, направленные на легализацию (отмывание) доходов, полученных преступным путем, и финансирование терроризма.

7.0.15. Другие страны

В ряде стран, например, во Франции и Индии, пока не было официального решения о регулировании и правовом статусе биткойна, однако регуляторы сделали заявления о том, что они пытаются выработать позицию в отношении криптовалют, и предупреждают потенциальных пользователей о высоких рисках вложений средств в криптовалюты из-за высокой волатильности[123]. Французский Центробанк считает, что даже профессиональные трейдеры должны быть осторожны — конвертируемость бит-

койна не гарантируется, держатель биткойнов вряд ли сможет обратиться в суд в случае воровства или мошенничества[12].

8. Альтернативы использования технологии

Открытый исходный код программного обеспечения системы Биткойн был использован для создания других систем:

- сети Namecoin — валюты и, одновременно, системы альтернативных корневых DNS-серверов.
- Форка «Litecoin», в котором используется функция хеширования scrypt вместо SHA-256, объём и скорость эмиссии увеличены в 4 раза, время подтверждения транзакций в 4 раза уменьшено.
- Форка «Primecoin», в котором в качестве системы подтверждения используются не хеши, а цепочки простых чисел. Это первый форк, в котором в качестве доказательства проделанной работы проводятся полезные вычисления.

9. Особенности

9.1. Неравенство между ранними и поздними майнерами

Правила эмиссии биткойнов дали больше преимуществ тем, кто занялся майнингом при небольшой совокупной мощности сети. Так, количество работы, необходимое для генерации блока, в настоящее время (2013 год) более чем в полмиллиона раз больше, чем в начале работы системы. При увеличении суммарной вычислительной мощности майнеров генерация становится более энерго- и аппаратнозатратной. Это сопровождается запланированным уменьшением размера награды за майнинг.

9.2. Резкие скачки курса

В середине 2011 года из-за спекулятивного спроса курс резко вырос до более чем тридцати долларов США, после чего упал примерно до двух долларов за биткойн. В течение 2012 года наблюдалась тенденция к росту, которая ускорилась в начале 2013 года. В апреле произошёл новый резкий подъём и последующий обвал. Значительные колебания курсов вызвали много обсуждений.

Так как эмиссия биткойнов ограничена (как по скорости, так и по общей сумме) и общее их количество никогда не превысит 21 млн, ряд авторов считают, что у людей есть стимул к спекулятивному накоплению биткойнов[124], исходя из предположения, что ограниченное предложение будет подталкивать курс к постоянному росту.

9.3. Теневая экономика

Возможность анонимности и неподконтрольность национальным органам власти привлекает к биткойну теневой экономический оборот. Хотя наличные деньги тоже могут использоваться анонимно и сделки с ними также неконтролируемы, биткойны пригодны для быстрых удалённых платежей.

Благодаря анонимности владельцев кошельков, биткойны получили популярность при покупке нелегальных товаров (в том числе наркотиков)[125][126], отмывания денег, добытых преступным путём[127]. Например, авторы вируса-ransomware CryptoLocker, шифрующего файлы, вымогали с пострадавших выкуп в биткойнах; общая полученная ими сумма за последний квартал 2013 года оценивается в несколько десятков миллионов долларов.[128]

9.4. Воровство

Так как в системе Биткойн нет контролирующего центра, невозможно обжаловать и/или отменить несанкционированные транзакции. Если оплата произведена, но услуга или товар не получены, также нет гарантий возврата платежа.

Опасным является кража файлов с ключами/адресами (wallet.dat). Если кошелек не зашифрован, злоумышленник может получить возможность перевода всех средств по своему усмотрению.

Уже были зафиксированы взломы площадок биткойн-бирж и пулов совместной добычи[129][130][131][132].

В конце 2013 года в СМИ появилась информация, что с транзитных счетов подпольного магазина Sheep Marketplace было украдено 96 000 биткойнов, принадлежавших пользователям[133][19]. Позже выяснилось, что официально сообщалось только о краже 5400 BTC, а кошелёк с 96000 BTC, который по предположению пользователей Reddit принадлежал злоумышленнику, оказался кошельком биткойн-биржи, через которую злоумышленник продал биткойны[134].

9.5. Скрытый майнинг

Для генерации биткойнов было возможно использование работниками корпоративных ресурсов, до массового появления ASIC майнинга.

В июне 2011 года Symantec заявила, что майнинг может быть запущен на ботнетах. В отчёте за второй

квартал 2011 года Лаборатория Касперского сообщила о троянском модуле, который занимался скрытым майнингом[135].

В апреле 2013 была зафиксирована крупная эпидемия вирусного распространения через текстовые сообщения в Skype троянских программ, цель которых поиск и кража файлов wallet.dat и скрытый майнинг на CPU[136][137].

При установке торрент-клиента µTorrent (версия 3.4.2 build 28913 и позднее) предлагается установить дополнительную программу EpicScale, которая позволяет использовать ресурсы компьютера во время простоя для распределённых вычислений. В настоящее время сеть EpicScale используется для майнинга биткойнов. Представители µTorrent заверяют, что часть полученных средств идут на финансирование компании, часть — на благотворительность[138].

9.6. Требование к дисковому пространству

Из-за особенностей функционирования системы объём информации, которую должен хранить и обрабатывать каждый пользователь стандартного клиента «Bitcoin-qt», постоянно растёт. По состоянию на октябрь 2014 года необходимый объём превышает 25 ГБ. На загрузку и формирование базы данных с нуля может уходить более суток из-за огромного количества мелких дисковых операций. В случае роста популярности и увеличения числа транзакций до уровней, сравнимых с популярными ныне платёжными системами, проблема хранения и передачи данных может сделать невозможным использование биткойнов на большинстве обычных домашних компьютеров. По этой причине разработаны «тонкие клиенты», которые хранят на жестком диске лишь их заголовки, а содержимое блоков скачивают только по мере необходимости. С их помощью можно пользоваться платёжной системой, но при этом они не подойдут для работы пула, соло-майнинга или майнинга на пуле «P2Pool».

10. Критика

Нет централизованного органа, выпускающего биткойны и осуществляющего контроль оборота. Каждый человек, на оборудовании которого выполняется работа по формированию новых блоков (майнинг), имеет шанс получить очередную порцию новых биткойнов.

10.1. Эмиссия денег вне контроля

Министерство финансов Российской Федерации в лице замминистра Алексея Моисеева предостерегает, что «существуют значительные риски бесконтрольной эмиссии „альтернативных“ денег, которая при свободном перетоке из легальной валюты и обратно может привести к потере контроля за денежным оборотом, отмыванию денег, мошенничеству»[139].

Банк Англии опасается за финансовую стабильность своей страны если у системы Биткойн увеличится популярность и не будет регулирования. Крайний вариант: если все внегосударственные платежи (например, кроме оплаты налогов), будут происходить через биткойны, то это приведёт к фрагментации экономики, а Банк Англии потеряет контроль над инфляцией[140].

Обвал цен на биткойны может повредить финансовой системе, если цифровые валюты будут использоваться в крупных сделках — например, на фондовых рынках. Крупные покупки цифровой валюты большим финансовым учреждением поставят в зависимость от перепадов цен многих участников рынка, даже если они не являются держателями криптовалюты.

10.2. Потеря контроля над денежными потоками

Псевдонимность системы Биткойн мешает государству контролировать финансовые потоки, в том числе через границу. Уже известны случаи отмывания денег с использованием биткойнов.

10.3. Оборот нелегальных товаров

Государство не может ограничивать операции купли-продажи за биткойны запрещенных товаров, таких как оружие, наркотики и т. д., так как трудно узнать, от кого именно и к кому переводятся средства.

10.4. Мнение о том, что Биткойн — не валюта

В интервью радио «Голос России» финансовый эксперт и американский предприниматель Карл Деннингер (англ. *Karl Denninger*) заявил, что биткойн никогда не был валютой, потому что для этого необходимо выполнение двух условий.

> Первое — необходимо быть средством обмена, чтобы вы и я могли совершать операции с различными товарами и услугами. А это требует повсеместного признания. Второе — необходимо быть стабильным

средством сохранения стоимости, таким, чтобы я мог вложить определенный объём своих экономических усилий в данную валюту и получить её обратно через время.

Оригинальный текст (англ.)

First, it needs to be a medium of exchange so you and I can transact in various goods and services. That requires wide acceptance. It also needs to be a stable store of value so that I can place a certain amount of value from my economic efforts into that particular currency and retrieve it at a later date.

— Карл Деннингер. Биткойн не валюта[141]

Уоррен Баффет считает, что биткойн не является долговечным средством обмена.

Это не валюта. Я бы не удивился, если бы его [биткойна] не было в ближайшие 10-20 лет.

Оригинальный текст (англ.)

It's not a currency. I wouldn't be surprised if it wasn't around in the next 10-20 years.

— Уоррен Баффет. I'm Buying Stocks If They Fall Today, And Bitcoin Is Not A Currency[142]

Вице-президент по мобильным разработкам компании DataArt Денис Марголин пишет, что биткойн «является отчасти услугой по анонимизации платежей, а отчасти — ценной бумагой, не подверженной никаким регуляциям, с весьма небольшим объёмом эмиссии, ставшей поэтому идеальной целью для спекуляций». По мнению Дениса Марголина биткойн — это не валюта; отмечая, что у криптовалюты нет будущего, он говорит, что это лишь «вера в чистый новый мир, лишенный влияния правительств и корпораций, левоанархистское технократическое общество, в котором наконец все будет устроено так, как кажется разумным» (меритократия).

10.5. Риски

Существует ряд недостатков системы Биткойн, которые также сказываются на майнерах.

На одном из российских ресурсов посвященном биткойну говорится о том, что это неподходящее решение для тех, кто ищет стабильности. «На данный момент курс биткойна нестабилен и нет уверенности, что завтра он будет стоить столько же, сколько и сегодня»[143].

Управляющий партнер юридической консалтинговой компании Артем Толкачев также ставит под сомнение надежность хранения криптовалюты, сообщая о прецеденте кражи 25 000 биткойнов с виртуального счета одного пользователя в 2011 году[144].

Центробанк РФ предостерегает россиян от использования биткойнов: «По „виртуальным валютам“ отсутствует обеспечение и юридически обязанные по ним субъекты. Операции по ним носят спекулятивный характер, осуществляются на так называемых „виртуальных биржах“ и несут высокий риск потери стоимости»[145].

Основная проблема биткойна заключается в том, что его воспринимают не как валюту и средство осуществления операций, а как объект инвестиций. Об этом свидетельствует сокращение количества транзакций в биткойнах[146]. Ограниченность запасов этой криптовалюты стимулирует людей накапливать её, а не тратить[147].

Джеймс Суровецки (англ. *James Surowiecki*), экономический обозреватель The New Yorker, считает, что благодаря стремительному росту ценности, а вместе с тем и популярности, система Биткойн выглядит как классический пузырь[148].

Но главное, люди решили, что покупать и держать биткойны — легкий способ зарабатывать деньги. В результате многие — вероятно, даже большинство — пользователей приобретают биткойны не для покупки товаров и услуг, а для спекуляции. Это плохое инвестиционное решение, которое к тому же плохо сказывается на перспективах биткойна.

Оригинальный текст (англ.)

More important, it also made people think that buying and holding bitcoins was an easy way to make a buck. As a result, many—probably most—Bitcoin users are acquiring bitcoins not in order to buy goods and services but to speculate. That's a bad investment decision, and it also hurts Bitcoin's prospects.

11. Интересные факты

- URI-схема «*bitcoin:*» официально включена в спецификации WHATWG для HTML5[149][150].
- До версии 0.8.0 для хранения цепочки блоков основной клиент использовал Berkeley DB, начиная с версии 0.8.0 разработчики перешли на LevelDB[151].
- Минимальную передаваемую величину 10^{-8} биткойн называют «сатоси» — в честь создателя Сатоси Накамото, хотя сам он использовал для обозначений минимальной передаваемой величины слово «цент»[152].

- 22 ноября 2013 года компания Virgin Galactic объявила о возможности оплатить через биткойн туристические суборбитальные космические полёты. Первой купила полёт с помощью биткойнов бортпроводница с Гавай, США[153][значимость факта?].

- В конце ноября 2013 года на BBC прошёл сюжет о британце, который начал проводить время на местной свалке в поисках выброшенного им же компьютерного жесткого диска. Оказалось, что на диске хранились 7,5 тыс. биткойнов, полученные им ещё в 2009 году. Диск не использовался на протяжении трёх лет, британец был уверен, что всё нужное с диска скопировано, и выбросил его. Из новостей он узнал о значительном росте курса биткойна и «осознал, что натворил». На момент «раскопок» стоимость информации на выброшенном винчестере превысила 7,5 млн долларов[154][19].

- 17 января 2014 года некоммерческий проект OpenBSD, код которого доступен под лицензией ISC, оказался под угрозой закрытия из-за того, что у канадского энтузиаста Тео де Раадта, занимающегося проектом и использующего для тестирования много различного оборудования у себя дома, накопилась задолженность за электроэнергию, эквивалентная 20000 долларов. Энтузиаст опубликовал письмо с просьбой о помощи[155][156]. Спонсор из числа биткойн-богачей, румынский предприниматель Мирча Попеску, сообщил, что готов пожертвовать сразу всю необходимую сумму[157][158][159][160].

- Ряд российских СМИ ошибочно[161] назвали сооснователя Bitinstant, обвинённого властями США в том, что не сообщал о подозрительных транзакциях[162], «создателем биткойн»[163].[значимость факта?]

- Компания SmartMetric объявила о доступности для предпринимателей и разработчиков платёжной карты со встроенным нанокомпьютером, которая является оффлайновым хранилищем биткойнов и совместима с имеющимися стандартами банкоматов[164].

- На игре Университетской лиги США один из студентов развернул плакат «Мама, пришли денег!». На плакате кроме этого призыва в объективы телекамер попал нарисованный знак биткойна и QR-код биткойн-кошелька студента. За сутки студент получил пожертвований биткойнами на 20 тысяч долларов[19].

- В одном из выпусков мультсериала The Simpsons, клоун-бизнесмен Красти жалуется на то, что «потерял все свои деньги, играя на биткойн-рынке»[19].

- Калифорнийский фотограф Меган Миллер представила серию фотографий, на которых запечатлела физические воплощения биткойна, чтобы показать людям, что это «не просто абстракция сложного технологического мира»[165].

12. См. также

- Криптоанархизм
- Свободный банкинг
- Litecoin
- Primecoin
- Zerocoin
- Bitmessage
- Хавала

13. Примечания

[1] https://bitcointalk.org/?topic=1756.0

[2] *Лопатников Л. И.* Биткойн // Словарь Лопатникова

[3] *Каррыев Б.* Биткойн // ИТ-революция: Хроники 1904—2013

[4] http://spar.isi.jhu.edu/~{}mgreen/ZerocoinOakland.pdf

[5] bitcoin: definition of bitcoin in Oxford dictionary

[6] *Кирилл Сарханянц, Ольга Шестопал, Роман Рожков* Много денег из ничего // Газета «Коммерсантъ», № 102/П (5133), 17.06.2013

[7] How Cryptocurrencies Could Upend Banks Monetary Role — Bank Think Article — American Banker

[8] Журнал Forbes: Виртуальный золотой стандарт: Некоммерческий проект Bitcoin собирается создать цифровую валюту, защищенную от инфляции

[9] Курс Bitcoin превысил $100 за 1 BTC

[10] Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity (англ.) — Отчёт ФБР о виртуальной валюте Биткойн; Краткий пересказ на русском

[11] Информация Банка России «Об использовании при совершении сделок „виртуальных валют“, в частности, Биткойн»

[12] Центробанки мира высказываются насчет Биткойна

[13] Американские регуляторы возьмутся за виртуальную валюту

[14] Банк в стиле киберпанк

[15] Вэй Дай Описание протокола криптовалюты «b-money» (англ.) (есть неофициальный перевод на русский)

[16] *Сергей Козловский* Никто не знает, но стоит дорого

[17] Bitcoin: Peer-To-Peer Electronic Cash System (англ.)

[18] Questions about Bitcoin

[19] *Виктор Фомин.* Сокровища ботанов: все, что важно знать о валюте будущего — биткоинах. *MAXIM* (февраль 2014). Проверено 26 августа 2014.

[20] *Eric Mack.* The Bitcoin Pizza Purchase That's Worth $7 Million Today (англ.), *Forbes* (12/23/2013). Проверено 27 августа 2014.; перевод *portwein74.* Пицца стоимостью 7 миллионов долларов. *Bit•Новости* (25 декабря 2013). Проверено 26 августа 2014.

[21] «Bitcoin: Peer-To-Peer Electronic Cash System» раздел № 11 «Calculations»

[22] Виртуальный золотой стандарт | Forbes.ru

[23] Онлайн-конференция «Биткоин: переходим на электронные деньги»

[24] *Nathan Willis.* Bitcoin: Virtual money created by CPU cycles, *LWN.net* (10 ноября 2010).

[25] Адреса Bitcoin. Часть 1, теория

[26] (англ.)

[27] «Bitcoin: Peer-To-Peer Electronic Cash System» раздел № 6 «Incentive»

[28] Обратимые транзакции в Bitcoin

[29] Биткойн — это финансовая платформа с разнообразными API // Bit•Новости

[30] *Satoshi Nakamoto.* Bitcoin: A Peer-to-Peer Electronic Cash System (1 августа 2011).

[31] Аннотация в «Bitcoin: Peer-To-Peer Electronic Cash System»

[32] «Bitcoin: Peer-To-Peer Electronic Cash System»: 7. Reclaiming Disk Space

[33] «Bitcoin: Peer-To-Peer Electronic Cash System»: 2. Transactions

[34] Transactions — Bitcoin

[35] Bitcoin Qt 0.6 Changelog

[36] Транзакции Bitcoin

[37] Bitcoin Block Explorer - сайт, позволяющий просматривать цепочку блоков. Архивировано из первоисточника 15 июля 2012.

[38] Статья о вероятности Double Spending атаки. Архивировано из первоисточника 21 мая 2013.)

[39] ASIC Mining Profits Will Be Gone By Summer (англ.). Bitcoin Insight (MARCH 24, 2013). — «January of this year the total hashrate of the Bitcoin network was less than 25 THash/s. In less than 3 months that figure has ballooned to more than 55 THash/s. The sharp increase is the result of newly available ASIC Bitcoin mining hardware» Проверено 30 ноября 2013.

[40] Bitcoin network reaches 2 Petahash/s - 2000 Thash/s (англ.). Cloudbitcoinminer (October 15, 2013). Проверено 30 ноября 2013.

[41] Bitcoin Charts

[42] https://www.btcguild.com/index.php?page=rankings Fastest Users (Last Hour) 269032 99,730.90 GH/s

[43] Bitcoin Clock, прогноз моментов изменения сложности и уменьшения вознаграждения

[44] Block 210000, Bitcoin Block Explorer

[45] http://www.theregister.co.uk/2011/08/16/gpu_bitcoin_brute_forcing/ «the idea of GPGPU extremely attractive for the purpose of bitcoin mining»

[46] http://arstechnica.com/tech-policy/news/2011/08/symantec-spots-malware-that-uses-your-gpu-to-mine-bitcoins.ars «estimates that GPUs can compute hashes up to 750 times as quickly as a typical CPU.»

[47] Графики изменения сложности сети Bitcoin

[48] http://blockexplorer.com/rawblock/0000000000000079d4636e1ed808c4f4b1b0f512ac74b4659e67b5f2a402c9a

[49] Pooled Mining //Bitcoin wiki

[50] Reward systems //Bitcoin wiki

[51] Mining pool reward FAQ //Bitcoin wiki

[52] bitcoin/bitcoin · GitHub

[53] Coins generated aren't considered confirmed by the Bitcoin protocol for 100 blocks. It is advisable to wait some additional time for a better chance that the transaction will be propogated by all nodes. The classic bitcoin client won't show generated coins as confirmed until the 120th block.

[54] https://en.bitcoin.it/wiki/Transaction_fee

[55] Спецификация API

[56] Библиотека классов для PHP5

[57] BitcoinJ на Google Code

[58] Google releases open source Bitcoin client — open source, money, Google, Gavin Andresen, Economics, e-commerce, Bitcoin — Java — Development — Techworld

[59] Bitcoin Trade. Bitcoin.org. Проверено 16 мая 2011.

[60] Donate to ReactOS — ReactOS Website

[61] Donate to WikiLeaks

[62] Download music, movies, games, software! The Pirate Bay — The galaxy's most resilient BitTorrent site

[63] Donate to EFF | Electronic Frontier Foundation

[64] Internet Archive Frequently Asked Questions

[65] Друскининкайский гостевой дом привлёк иностранцев необычной формой расчёта

[66] Биткойн и основы фьючерсной торговли. Проверено 28 июня 2013. Архивировано из первоисточника 1 июля 2013.

[67] Online-Only Currency BitCoin Reaches Dollar Parity

[68] «Crypto Currency»

[69] «The Underground Website Where You Can Buy Any Drug Imaginable» (англ.)

[70] The Rise and Fall of Bitcoin

[71] Bitcoin Charts / Charts. Проверено 26 февраля 2013. Архивировано из первоисточника 13 марта 2013.

[72] CLARIFICATION OF MT. GOX COMPROMISED ACCOUNTS AND MAJOR BITCOIN SELL-OFF

[73] Bitcoin Charts / Charts. Проверено 20 апреля 2013. Архивировано из первоисточника 29 апреля 2013.

[74] Bitcoin Charts / Charts. Проверено 20 апреля 2013. Архивировано из первоисточника 29 апреля 2013.

[75] Bitcoin Charts / Charts. Проверено 20 ноября 2013.

[76] Bitcoin Charts / Charts. Проверено 28 ноября 2013.

[77] Wayback Machine: Mt Gox. Проверено 12 апреля 2013.

[78] Mt. Gox Trading Halts As Bitcoin Businesses Move to Assure Investors

[79] The Coinbase Blog — Joint Statement Regarding MtGox

[80] Винклвоссы рассчитали свой индекс стоимости Bitcoin

[81] *Karpeles, Mark.* [illegible] / Announcement regarding the balance of Bitcoin held by the company (яп.) (PDF). MtGox (20 марта 2014). — «MtGox Co., Ltd. had certain oldformat wallets which were used in the past and which, MtGox thought, no longer held any bitcoins. Following the application for commencement of a civil rehabilitation proceeding, these wallets were rescanned and their balance researched. On March 7, 2014, MtGox Co., Ltd. confirmed that an oldformat wallet which was used prior to June 2011 held a balance of approximately 200,000 BTC (199,999.99 BTC).» Проверено 22 марта 2014. Архивировано из первоисточника 22 марта 2014.

[82] beCoin — Биткоин Лайткоин Аналитика Новости — Mt.Gox подала заявление о ликвидации

[83] WMX — новый тип титульных знаков

[84] «An Analysis of Anonymity in the Bitcoin System»

[85] Почему Биткоин так важен? / Блог компании Хост-Трекер / Хабрахабр

[86] http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/

[87] Что такое криптовалюта / ДИАЛОГ.ua

[88] Япония изучает Bitcoin

[89] Everyone Is Baffled By Alan Greenspan's Comment About Bitcoin

[90] Герман Греф о криптовалютах в Давосе | New Money Feed

[91] Греф обяжет Сбербанк принимать биткойны? — Избранное — Полит-онлайн

[92] Кэмерон Уинклвосс прогнозирует рост курса биткойна до 40 тыс. долларов | Лента новостей | Банки.ру

[93] Venture Capitalist Chris Dixon Believes Bitcoin Will Hit $100k

[94] Германия признала Bitcoin

[95] Croatia considers Bitcoin legal; 45 members of the Swiss parliament want the same | BitCoin Examiner

[96] Denmark's Authorities: Bitcoin is Not Regulated Here

[97] Mervärdesskatt: Handel med bitcoins — Skatterättsnämnden

[98] Good news regarding Bitcoin and VAT in Sweden

[99] Korea Announces Favorable Tax Policy for BTC | Bitcoin Babble

[100] Власти Японии готовы обложить операции с биткойном налогом. Интерфакс (5 марта 2014). Проверено 21 марта 2014.

[101] Trading suspended due to Bank of Thailand advisement

[102] Возвращение Bitcoin в Таиланд — Cryptorise

[103] Банк Таиланда опять против — Cryptorise

[104] ЦБ Китая запретил банкам операции с Bitcoin

[105] PBOC Rule Means Bitcoin Websites in China Must Close, Expert Says — Caixin Online

[106] Virtual Correncу Schemes (англ.). European Central Bank (October 2012). Проверено 2 ноября 2012. Архивировано из первоисточника 5 ноября 2012.

[107] Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies

[108] FinCEN guidance on virtual currencies

[109] Hearings: Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies

[110] Court officially declares Bitcoin a real currency // RT USA, August 09, 2013

[111] IRS Notice 2014-41

[112] Рецепт налогообложения биткоина от США / TAX-TODAY.COM

[113] Etablir la sécurité juridique concernant le bitcoin

[114] Сингапур планирует легализовать Bitcoin

[115] Singapore government to tax some bitcoin transactions

[116] Сингапур урегулировал налогообложение операций с Bitcoin — Taxpravo.ru

[117] Сингапур признал биткоин и определил налоговую политику его оборота — TJournal

[118] MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks — Monetary Authority of Singapore

[119] Доходите от сделки с биткойн се декларират и облагат — Национална Агенция за Приходите

[120] *Георгий Лунтовский.* ЦБ признал, что у биткоина может быть будущее в России. ИТАР-ТАСС (2 июля 2014 года).

[121] Портал о биткоинах попал в список запрещенных в России сайтов // Лента.ру 13 января 2015

[122] решения Невьянского городского суда Свердловской области 30 сентября 2014 года

[123] Индия присматривается к Bitcoin

[124] Technical Analysis in the Virtual World. Philip Daniel «As bitcoins deflate and gain value relative to other currencies, those holding bitcoins become more wealthy. As deflation happens the incentive to hold bitcoins and not spend them increases. This could hurt the bitcoin economy»

[125] *Fernholz, Tim* Silk Road collected 9.5 million bitcoin—and only 11.75 million exist. QUARTZ (2 октября 2013). — «the currency's primary use so far (besides as a speculative investment vehicle and point of departure for futuristic payment schemes) was buying illegal things online.» Проверено 10 октября 2013.

[126] *RAFFAELA WAKEMAN.* "Take the Drugs, But Don't Take the People's Bitcoins", *New Republic* (OCTOBER 9, 2013). Проверено 21 октября 2013. «(To date, the world has about 11.75 million bitcoins, each worth as of this writing $137 from a variety of sources.) Note that Silk Road's revenue prior to being shut down was 9.5 million bitcoin—meaning that nearly all of the virtual currency that's been generated thus far worldwide was being spent on this system.».

[127] *JIM EDWARDS.* CLAIM: Bitcoin Is Basically For Criminals (англ.), *Business Insider* (NOV. 27, 2013). Проверено 4 декабря 2013.

[128] *Violet Blue.* CryptoLocker's crimewave: A trail of millions in laundered Bitcoin (англ.), *ZDNet* (December 22, 2013). Проверено 23 декабря 2013.

[129] BTC-E | News

[130] Хакерская атака на Mt Gox

[131] Взломаны сервера на Linode, украдено около 50K BTC ($250K) / Хабрахабр

[132] Кража 24,000 BTC у Bitfloor

[133] *JIM EDWARDS.* A Thief Is Attempting To Hide $100 Million In Stolen Bitcoins — And You Can Watch It Live Right Now (англ.), *Business Insider* (DEC. 3, 2013). Проверено 4 декабря 2013. «A person who allegedly robbed the web site Sheep Marketplace of 96,000 Bitcoins — about $100 million at current prices — is attempting to hide the heist».

[134] Цифровая погоня за золотым гусём, или как самая большая афера в истории Bitcoin превратилась в фарс / Хабрахабр

[135] Развитие информационных угроз во втором квартале 2011 // Лаборатория Касперского

[136] Троян в Skype использует компьютер жертвы для генерирования Bitcoin | информационный портал по безопасности. Проверено 17 апреля 2013.

[137] Skypemageddon by bitcoining, An avalanche in Skype // Dmitry Bestuzhev (Kaspersky Lab), 4 April 2013;
Новый skype-троян превращает компьютер в раба, добывающего Bitcoin / Хабрахабр. Проверено 17 апреля 2013. Архивировано из первоисточника 18 апреля 2013.

[138] What is Epic Scale? (англ.)

[139] Минфин предложил ввести штрафы за использование биткоинов // «Ведомости» 06.10.2014

[140] Банк Англии: В будущем биткоины могут пошатнуть финансовую стабильность Великобритании — Apparat

[141] *Карл Деннингер* Bitcoin не валюта // Интервью «Голос России 21.02.2014 (англ.)

[142] *Уоррен Баффет* I'm Buying Stocks If They Fall Today, And Bitcoin Is Not A Currency (англ.)

[143] First Bitcoins

[144] Возможности и риски использования биткоин в России. Юридический анализ цифровой валюты

[145] Об использовании при совершении сделок «виртуальных валют», в частности, Биткойн

[146] Количество транзакций в биткоинах снизилось. | Cryptobit

[147] Cryptocurrency | MIT Technology Review

[148] «Взамен валют» — Журнал Esquire

[149] Схему URI для платежей Bitcoin добавили в стандарт HTML5 // Xakep.ru, 24.04.2013

[150] HTML5, A vocabulary and associated APIs for HTML and XHTML. W3C Candidate Recommendation // W3C, 6 August 2013 «The following schemes are the whitelisted schemes: bitcoin»

[151] Релиз Bitcoin 0.8.0 - OpenSource - Новости. Проверено 22 февраля 2013. Архивировано из первоисточника 13 марта 2013.

[152] Bitcoin: Peer-To-Peer Electronic Cash System”: 9. Combining and Splitting Value

[153] Bitcoins in space. Virgin (November 22, 2013). Проверено 22 ноября 2013.

[154] Британец выбросил жесткий диск с биткоинами на $7,5 млн

[155] Electricity bill threatens survival of OpenBSD | ZDNet

[156] Проект OpenBSD под угрозой закрытия: нет денег на оплату счетов за электричество / Хабрахабр

[157] #bitcoin-assets log

[158] #bitcoin-assets log

[159] Румынский биткоин-миллионер оплатил долги OpenBSD / Хабрахабр

[160] OpenBSD Project survived after $20,000 Donation from Romanian Bitcoin Billionaire — The Hacker News

[161] Lenta.ru: Интернет и СМИ: Интернет: Российские СМИ объявили главу биткоин-биржи создателем биткоинов

[162] В США арестовали вице-председателя Bitcoin Foundation

[163] В США арестован создатель виртуальной валюты биткойн Чарли Шрем — Первый канал

[164] SmartMetric предлагает карту для расчетов в Bitcoin и используемую в ней сверхмалую операционную систему для нанокомпьютеров // IXBT

[165] Реальные деньги: Фотографии биткоинов в мире вещей — Apparat

14. Литература

- *Виктор Фомин* Деньги: план ฿ // *MAXIM* : журнал. — 2014. — № 143. — С. 82—87. — ISSN 1682-8976.

15. Ссылки

- Официальный сайт
- Русскоязычный информационный ресурс о сети Bitcoin
- Курсы биткойна на крупных площадках обмена
- Карта мест где принимают биткойны
- Bitcoin: The political ‘virtual’ of an intangible material currency // International Journal of Community Currency Research VOLUME 17 (2013) SECTION A 8-18
- Графики изменения сложности/мощности сети
- Сравнение оборудования пригодного для эмиссии биткойнов, Bitcoin wiki
- Евгений Золотов BitCoin как убежище: стоит ли вложиться в криптовалюту? // I-business, 21 июня 2012
- Пол Форд Биткойн может оказаться последней «безопасной гаванью» глобальной экономики перевод статьи Bitcoin May Be the Global Economy’s Last Safe Haven // BloombergBusinessweek, March 28, 2013
- Сергей Козловский Мир братьев-коинов // Lenta.ru, 18 декабря 2013
- Сергей Голубицкий — Монеты и симулякры // Бизнес-журнал, 18 Января 2014

16. Источники текстов и изображения, авторы и лицензии

16.1. Текст

- **Биткойн** *Источник:* http://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82%D0%BA%D0%BE%D0%B9%D0%BD?oldid=69264231 *Авторы:* Nashev, Dodonov, Sindicollo, Hayk, YurikBot, Выползень, Gruznov, A5b, Kink, Rushka, ZhN, Sentinel.ru, PBot, Vasiley, Knyf, Nickispeaki, Marcus Cyron, Klip game, РоманСузи, Vs64vs, Tyratam, M0Ray, Chelovechek, Mcherenkov, Alex.ryazantsev, UncleMartin, Calibrator, Catherine Sh, Hellerick, Vlsergey, Niklem, Kabatov, Analyzer (KODEP), HORD, Adamant-GEO, Alexbyk, Ле Лой, KOLANICH, Inc ru, Козырь, Jackie, Dextran, Aleksey Bragin, Vituzzu, Zorrobot, Серж Тихомиров, ANATHEM, LaaknorBot, ArjLover, Forajump, Amirobot, MystBot, Luckas-bot, SF007, Филатов Алексей, Ecureuil espagnol, Rubinbot, PositiveSky, Zukel, ArthurBot, Rschen7754, 4th-otaku, Bechamel, Okras, Yurymik, Bloodmage2, Кубаноид, Westsomething, Иван Волкотруб, Melksoft, Middle urals, LucienBOT, Kalashnov, Sigwald, TwoPizza, Zenixan, Flint1972, IlyaVak, Wargasm, Tegel, Dmitry89, Freeneutron, Vort, Hupia, VAP+VYK, RedBot, Biathlon, Krassotkin, Dunay, Trolzen, Igorus77, Dmitru, Ripchip Bot, Calibrux, Mvk608, EmausBot, Arbnos, Arsen.Shnurkov, IKBAHT, Cfr, Deepak-nsk, ZéroBot, Atticagirl, Disem, Mekadva, Seomarlboro, Trititaty, Allez-ru, OneLittleMouse, Evgen Bodunov, El-chupanebrej, MaxBioHazard, Вовчик86, MGriBot, Wikifido, ChuispastonBot, H2Bot, WikitanvirBot, Arnekwiki, Arthur Ignatyev, Cinemantique, Movses-bot, KrBot, OverQuantum, WebCite Archiver, Daemvil, Bryndin, MerlIwBot, W2Bot, Autumn Leaves, MBHbot, KPu3uC B Poccuu, Алексей Неботов, Sealle, Programman, Ecurrencies, ThisIsNotReal, Draa kul, Ivan.a.tikhonov, Sumej, Виктория Гладкова, Fedorkov Dmitry, Volovik Vitaly, Parviz555, 0x0F, Tersa River, BS-Alex, Akledirs, YFdyh-bot, Burzuchius, Astrik, Coinman, TheOldOne, Vla.kas, RotlinkBot, Sr.ganador, Dimaniznik, Слишком похожий, Roman Kerimov, BitcoinTools, Cryptcoin, Outlook2003, Akh81, BitKing, Cnc dev, Lindorenan4, JonDow, Mezrin, Tikhomipavel, Rty2013, Bobrov Andrey, Ghosto, AVProk, Zferdinandz, Gorvzavodru, Кот на крыше, Imunderfire, Bitcoin4currencycom, Ти44ер, Andwild, Lixta, Sing guru, PetrMiw, Citing Bot, Hannasnow, Mozzzus, Yaroslav11, Salym5, Artur sardaryan, UvAntVl, Q-bit array, AveSidjey, Arvicco, Aapxx87, Wooow-booow, Wikmeiser, RIS-PROJECT, Parmal7, ChainTime, Tonyredd и Аноним: 289

16.2. Изображения

- **Файл:Ambox_scales.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/5/5c/Ambox_scales.svg *Лицензия:* Public domain *Авторы:* self-made using inkscape and based off of Image:Emblem-scales.svg *Художник:* penubag and Tkgd2007 (scales image)
- **Файл:Arrange-boxes.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/94/Arrange-boxes.svg *Лицензия:* CC BY-SA 3.0 *Авторы:* собственная работа *Художник:* RRZE
- **Файл:Bitcoin-client-0.7.1.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/5/57/Bitcoin-client-0.7.1.png *Лицензия:* Public domain *Авторы:* собственная работа *Художник:* ru:Участник:Alex.ryazantsev
- **Файл:Bitcoin.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/46/Bitcoin.svg *Лицензия:* CC0 *Авторы:* Этот файл является производной работой от: Bitcoin logo.svg
  Художник: Bitboy
- **Файл:Bitcoin_exchange_BTC-e_log_scale.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/8/8a/Bitcoin_exchange_BTC-e_log_scale.png *Лицензия:* CC BY-SA 3.0 *Авторы:* http://bitcoincharts.com/charts/btceUSD#tgMzm1g10zm2g25zl *Художник:* http://bitcoincharts.com
- **Файл:Bitcoin_logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/c/c5/Bitcoin_logo.svg *Лицензия:* CC0 *Авторы:* Bitcoin forums *Художник:* Bitboy
- **Файл:Bitcoin_winkdex.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/8/85/Bitcoin_winkdex.png *Лицензия:* Public domain *Авторы:* http://winkdex.com *Художник:* Winklevoss twins
- **Файл:Blockchain.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/9/98/Blockchain.svg *Лицензия:* CC BY 3.0 *Авторы:* Bitcoin Wiki: https://en.bitcoin.it/wiki/File:Blockchain.png *Художник:*
  - original file: Theymos from Bitcoin wiki
  - vectorization: собственная работа
- **Файл:Commons-logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/4/4a/Commons-logo.svg *Лицензия:* Public domain *Авторы:* This version created by Pumbaa, using a proper partial circle and SVG geometry features. (Former versions used to be slightly warped.) *Художник:* SVG version was created by User:Grunt and cleaned up by 3247, based on the earlier PNG version, created by Reidab.
- **Файл:Searchtool.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/61/Searchtool.svg *Лицензия:* LGPL *Авторы:* http://ftp.gnome.org/pub/GNOME/sources/gnome-themes-extras/0.9/gnome-themes-extras-0.9.0.tar.gz *Художник:* David Vignoni, Ysangkok
- **Файл:Wiki_letter_w.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/6/6c/Wiki_letter_w.svg *Лицензия:* CC-BY-SA-3.0 *Авторы:* собственная работа *Художник:* Jarkko Piiroinen
- **Файл:Wikinews-logo.svg** *Источник:* https://upload.wikimedia.org/wikipedia/commons/2/24/Wikinews-logo.svg *Лицензия:* CC BY-SA 3.0 *Авторы:* This is a cropped version of Image:Wikinews-logo-en.png. *Художник:* Vectorized by Simon 01:05, 2 August 2006 (UTC) Updated by Time3000 17 April 2007 to use official Wikinews colours and appear correctly on dark backgrounds. Originally uploaded by Simon.
- **Файл:Wiktionary-logo-ru.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/bc/Wiktionary-logo-ru.png *Лицензия:* CC BY-SA 3.0 *Авторы:* Russian Wiktionary *Художник:* One half 3544, VPliousnine
- **Файл:total_bitcoins_over_time.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/5/54/Total_bitcoins_over_time.png *Лицензия:* CC BY 3.0 *Авторы:* https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png *Художник:* Insti

- **Файл:Модель_приватности_в_Bitcoin.svg** *Источник:* https://upload.wikimedia.org/wikipedia/ru/5/58/%D0%9C%D0%BE%D0%B4%D0%B5%D0%BB%D1%8C_%D0%BF%D1%80%D0%B8%D0%B2%D0%B0%D1%82%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%B2_Bitcoin.svg *Лицензия:* Общественное достояние *Авторы:* Перевод иллюстрации из технической спецификации Bitcoin *Художник:* Satoshi Nakamoto, 0x0F (перевод)
- **Файл:Транзакции.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/1/16/%D0%A2%D1%80%D0%B0%D0%BD%D0%B7%D0%B0%D0%BA%D1%86%D0%B8%D0%B8.png *Лицензия:* CC BY-SA 3.0 *Авторы:* Transferred from ru.wikipedia *Художник:*

  Original uploader was Vla.kas из русский Википедия.
- **Файл:Хэш_транзакций.png** *Источник:* https://upload.wikimedia.org/wikipedia/commons/b/b7/%D0%A5%D1%8D%D1%88_%D1%82%D1%80%D0%B0%D0%BD%D0%B7%D0%B0%D0%BA%D1%86%D0%B8%D0%B9.png *Лицензия:* CC BY-SA 3.0 *Авторы:* Transferred from ru.wikipedia
  Художник:

  Original uploader was Vla.kas из русский Википедия.

16.3. Лицензия